(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 965 445 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
09.03.2022 Bulletin 2022/10

(21) Application number: **19927153.7**

(22) Date of filing: **13.12.2019**

(51) Int Cl.:
H04W 12/00 *(2021.01)* ***H04W 12/08*** *(2021.01)*

(86) International application number:
PCT/CN2019/125051

(87) International publication number:
WO 2020/220694 (05.11.2020 Gazette 2020/45)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **29.04.2019 CN 201910355810**

(71) Applicant: **Huizhou TCL Mobile Communication Co., Ltd**
Guangdong 516006 (CN)

(72) Inventor: **ZHAO, Yunhua**
Huizhou, Guangdong 516006 (CN)

(74) Representative: **Petraz, Gilberto Luigi et al**
GLP S.r.l.
Viale Europa Unita, 171
33100 Udine (IT)

(54) ROUTER, NETWORK CONNECTION METHOD AND MOBILE TERMINAL

(57) Provided are a router, a network connection method and a mobile terminal. The network connection method comprises: a router receiving a first dynamic password from a server; the router receiving a second dynamic password from a mobile terminal, and performing matching on the basis of the second dynamic password and the first dynamic password; if the matching is successful, establishing a connection, and sending a first result signal to the mobile terminal; and the router purging connection information associated with the connection after the connection has been established. The invention can prevent an unauthenticated terminal from connecting to a router, thereby enhancing the security of a connection established by means of a router.

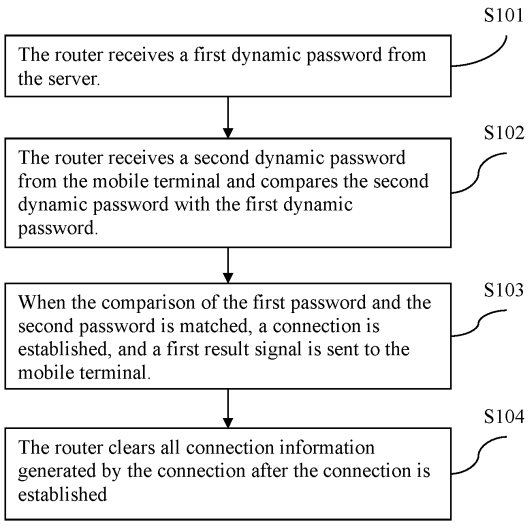

FIG. 1

EP 3 965 445 A1

Description

[0001] The present application claims the priority of a Chinese patent application with application No. 201910355810.1 and invention title "Router, mobile terminal, network connection method, and storage medium" submitted to the China National Intellectual Property Administration on April 29, 2019, which is incorporated by reference in the present application in its entirety.

FIELD OF THE INVENTION

[0002] The application relates to the field of intelligent communication technology, in particular, to a router, a network connection method, and a mobile terminal.

BACKGROUND

[0003] Inventors of the present application have found through long-term research and development that most current public WiFi connections are directly connected to a router using an unencrypted connection method. After browsing a login page or advertisement page provided by the router, the router allows a connecting terminal device to access the Internet. Since a preset key and a pairwise master key (PMK) of the router are fixed values, a large number of connection sessions remain active in the router for terminal devices in idle or without authorization from a login page on the router, resulting in slow router operation and poor Internet experience.

SUMMARY

Technical Problem

[0004] The main technical problem to be solved by the application is to provide a router, a mobile terminal, and a corresponding network connection method, so as to prevent resource consumption caused by excessive connection sessions of idle or unauthorized terminal devices.

Technical Solution

[0005] To solve the above technical problem, a technical solution adopted in the application is to provide a network connection method applicable to a router, comprising the following steps.

[0006] The router receives a first dynamic password from a server.

[0007] The router receives a second dynamic password from a mobile terminal and compares the second dynamic password with the first dynamic password.

[0008] When the comparison is matched, a connection is established, and a first result signal is sent to the mobile terminal.

[0009] The router clears connection information generated by the connection after the connection is established.

[0010] To solve the above technical problem, another technical solution adopted in the application is to provide a network connection method applicable to a mobile terminal, comprising the following steps.

[0011] The mobile terminal recognizes the image information from the router, and sends a first request signal to the server when the image information recognition is successful.

[0012] The mobile terminal receives a second dynamic password from the server.

[0013] The mobile terminal sends the second dynamic password to the router for verification.

[0014] The mobile terminal receives a first result signal from the router.

[0015] To solve the above technical problem, another technical solution adopted in the present application is to provide a mobile terminal, the mobile terminal comprises a memory and a processor interconnected with each other.

[0016] The memory stores program instructions.

[0017] The processor memory executes program instructions to carry out the following steps.

[0018] The mobile terminal recognizes the image information from the router and sends a first request signal to the server when the image information recognition is successful, wherein the image information comprises an identification code.

[0019] The mobile terminal receives a dynamic password from the server.

[0020] The mobile terminal sends a dynamic password to the router.

[0021] The mobile terminal receives a first result signal from the router.

[0022] To solve the above technical problem, another technical solution adopted in the present application is to provide a router, the router comprises a memory and a processor interconnected with each other.

[0023] The memory stores program instructions.

[0024] The processor memory executes program instructions to carry out the following steps.

[0025] The router receives a first dynamic password from the server.

[0026] The router receives a second dynamic password from the mobile terminal and compares the second dynamic password with the first dynamic password, wherein the second dynamic password is assigned to the mobile terminal by the server.

[0027] When the comparison is matched, a connection is established, and a first result signal is sent to the mobile terminal.

[0028] The router clears connection information generated by the connection after the connection is established.

[0029] To solve the above technical problem, another technical solution adopted in the present application is to provide a storage medium in which program data is stored in the storage medium, and the program data can be executed to implement the network connection method described above.

Advantageous Effects

[0030] In the network connection method proposed in the application, the mobile terminal identifies the image information of the router and sends a first request signal to the server, the router receives a first dynamic password from the server, the mobile terminal receives a second dynamic password from the router, the mobile terminal sends the second dynamic password to the router, and the router receives the second dynamic password. The second dynamic password is compared with the first dynamic password. When the comparison is matched, the connection is established and connection information generated by this connection is cleared when the connection is established, to prevent idle terminals from connecting to the router.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031]

FIG. 1 is a flowchart of a first embodiment of a router network connection method of the present application.

FIG. 2 is a flowchart of a second embodiment of the router network connection method of the present application.

FIG. 3 is a flowchart of a third embodiment of the router network connection method of the present application.

FIG. 4 is a flowchart of a first embodiment of a mobile terminal network connection method of the present application.

FIG. 5 is a flowchart of a second embodiment of the mobile terminal network connection method of the present application.

FIG. 6 is a flowchart of a third embodiment of the mobile terminal network connection method of the present application.

FIG. 7 is a structural diagram of signal transmission of the network connection method of the mobile terminal and the router of the present application.

FIG. 8 is a structural diagram of the mobile terminal/router of the present application.

FIG. 9 is a structural diagram of an embodiment of a storage medium of the present application.

DETAILED DESCRIPTION

[0032] The following descriptions may clearly and completely disclose the technical solution in the embodiment of the application in combination with the drawings in the embodiment of the application. Obviously, the described embodiments are only part of the embodiments of the application, not all the embodiments. Based on the embodiments of the application, all other embodiments obtained by ordinary technical personnel in the art without creative endeavor belong to the scope of protection of the application.

[0033] The terms "first", "second" and "third" in this application are only used for description purpose, and cannot be understood as indicating or implying relative importance or implicitly indicating the quantity of the indicated technical features. Thus, the features defined as "first", "second" and "third" may explicitly or implicitly include at least one of the features. In the description of the application, "multiple" means at least two, such as two, three, etc., unless otherwise specified. All directional indications in the embodiment of the application (such as up, down, left, right, front, back...) are merely used to explain the relative position relationships, motion situations, and etc. between the components under a certain attitude (as shown in the attached figure). If the specific attitude changes, the directional indication may change accordingly. In addition, the terms "include" and "have" and any variations thereof are intended to cover exclusive inclusions. For example, a process, method, system, product, or device that contains a series of steps or units is not limited to the listed steps or units, but may also include steps or units not listed, or may also include other steps or units inherent to these processes, methods, products, or equipment.

[0034] The reference to "Embodiments" herein means that specific features, structures, or features described in connection with the embodiments may be included in at least one embodiment of the present application. The presence of the phrase in various places in the specification does not necessarily refer to the same embodiment, nor is it an independent or alternative embodiment mutually exclusive with other embodiments. It is explicitly and implicitly understood by those skilled in the art that the embodiments described herein may be combined with other embodiments.

[0035] The present application is described in detail below in combination with the drawings and the embodiment.

[0036] Refer to FIG. 1, a flowchart of a first embodiment of a router network connection method of the present application is described in the following steps.

[0037] In step S101, the router receives a first dynamic password from the server.

[0038] Wherein, the first dynamic password is a password randomly assigned by the server, which can be a digital password, a combination of numbers and letters, such as "128963", "ad5263", etc.

[0039] In step S102, the router receives a second dynamic password from the mobile terminal and compares the second dynamic password with the first dynamic password.

[0040] The second dynamic password, in one embodiment, is the same as the first dynamic password, randomly assigned by the server. After the server receives the first request signal from the mobile terminal, the server may randomly generate a dynamic password which is then simultaneously sent to the mobile terminal and the router, respectively, so that the mobile terminal can conduct an identity verification with the router through the dynamic password. In this case, the mobile terminal sends the second dynamic password to the router for verification.

[0041] In step S103, when the comparison of the first password and the second password is matched, a connection is established, and a first result signal is sent to the mobile terminal.

[0042] After receiving the second dynamic password sent by the mobile terminal, the router compares the second dynamic password with the first dynamic password received from the server. If the results are inconsistent, the verification is failed so that the connection cannot be established. If the results are consistent, the verification is successful, allowing a connection to be established for the mobile terminal. A first result signal is therefore sent to the mobile terminal to prompt the mobile terminal that the network connection is established.

[0043] In step S104, the router clears all connection information generated by the connection after the connection is established.

[0044] After the connection is successful, the router may clear the dynamic password and information of the mobile terminal connected, such as the model and identification code of the mobile terminal, so that the mobile terminal cannot automatically establish a new connection when it enters the WiFi area next time.

[0045] Refer to FIG. 4, a flowchart of a first embodiment of a mobile terminal network connection method of the present application comprises the following steps.

[0046] In step S401: the mobile terminal recognizes the image information from the router and sends a first request signal to the server when the recognition of the image information is successful.

[0047] Wherein, the mobile terminal is a mobile phone, an iPad, and other electronic devices. The image information of the router can be an identification code information such as a two-dimensional code or a bar code, which identifies the address and factory information of the router. The mobile terminal can scan the image through a camera and other devices, and send a first request to the server after obtaining the information of the router from the scanning.

[0048] In step S402, the mobile terminal receives the second dynamic password from the server.

[0049] Wherein, the second dynamic password, in one embodiment, is the same as the first dynamic password in step S101, randomly assigned by the server. It can be a digital password, a combination of numbers and letters, such as "128963", "ad5263", etc.

[0050] In step S403, the mobile terminal sends a second dynamic password to the router.

[0051] After receiving the second dynamic password sent by the server, the mobile terminal sends the second dynamic password to the router, which is then verified by the router.

[0052] In step S404, the mobile terminal receives a first result signal from the router.

[0053] The router compares the second dynamic password with the first dynamic password upon reception of the second dynamic password from the mobile terminal. A connection is established when the first dynamic password and the second dynamic password are matched. A first result is sent to the mobile terminal so that when the mobile terminal receives the first result, the mobile terminal confirms that the connection is established.

[0054] The scheme proposed in this embodiment is summarized as follows. The mobile terminal recognizes the image information of the router, sends the first request signal to the server, then receives the second dynamic password from the server. The router receives the first dynamic password from the server, the mobile terminal sends the second dynamic password to the router, and the router compares the second dynamic password with the first dynamic password. When the comparison is matched, the connection is established. When the connection is established, all connection information generated by the connection is cleared, so as to prevent the performance hits caused by automatic establishment of unwanted new connections when the mobile terminal enters the WiFi area next time.

[0055] See FIG. 2, a flowchart of a second embodiment of the router network connection method of the application

comprises the following steps.

[0056] In step S201: the router receives the first dynamic password from the server.

[0057] As in the previous embodiment, the first dynamic password is a password randomly assigned by the server, which can be a digital password, a combination of numbers and letters, such as "128963", "ad5263", etc.

[0058] In step S202: the router generates a first master key according to the first dynamic password.

[0059] The method of generating the first master key by the router according to the first dynamic password is based on a well-known hash function PBKDF2_SHA1, shown as: PMK = PBKDF2_SHAl (first dynamic password, SSID, SSID length, 4096), where PMK denotes a master key, SSID denotes a router address, and PBKDF2_SHAl denotes a hash operation.

[0060] The pairwise master key (PMK) is a symmetric key that the applicant (i.e., the mobile terminal) and the authenticator (i.e., the router) can share a symmetric key called a pair of master keys, which is used to control the signal access between the two. According to the embodiment of the application, the PMK comes from the passwords, and in other embodiments, the PMK can be dynamically specified.

[0061] In step S203, the router generates the first random number and sends the first random number to the mobile terminal.

[0062] The first random number is generated by the router, and the router sends the first random number to the mobile terminal after generating the first random number. The mobile terminal is capable of generating a second random number, which may be sent to the router as a third random number.

[0063] In step S204, the router receives a third random number and the first temporary key from the mobile terminal, and generates a fourth random number.

[0064] Wherein, the fourth random number, like the third random number, is a randomly generated number. The fourth random number is different from the third random number and can only be used once.

[0065] In step S205, the router generates a second temporary key according to the third random number, the fourth random number, and the first master key.

[0066] The second temporary key is generated according to the third random number, the fourth random number, and the first master key in a pseudo-random function PRF-X, shown as:

$$PTK = PRF\text{-}X\ (PMK, \text{"pairwise key expansion"}), Min\ (AA, SA) \parallel Max(AA, SA) \parallel Min(ANonce, SNonce) \parallel Max(ANonce, SNonce)),$$

where PTK denotes the temporary key, ANonce denotes a random number generated by the router, SNonce denotes a random number generated by the mobile terminal, AA denotes an identification address of the router, SA denotes an identification address of the mobile terminal, PRF-X denotes the pseudo-random function, and the pairwise key expansion is a constant string.

[0067] It should be noted that when the mobile terminal sends the third random number to the router, it includes the Media Access Control or Medium Access Control (MAC) address of the mobile terminal, which is translated into media access control or physical address, hardware address, for defining the location of network equipment. In the Open System Interconnection/Open System Interconnection Reference Model (OSI/RM), the third network layer is responsible for the IP address and the second layer data link is responsible for the MAC address. Therefore, a host has a MAC address, and each network location has an IP address dedicated to it. The MAC address is determined by the network card and is fixed. The MAC address is the aforementioned identification address.

[0068] In step S206, the router compares the second temporary key with the first temporary key.

[0069] After calculating the second temporary key, the router compares the calculated second temporary key with the first temporary key received from the mobile terminal.

[0070] In step S207, when the second temporary key matches the first temporary key, a connection is established, and a second result signal is sent to the mobile terminal.

[0071] The router compares the second temporary key with the first temporary key. If the results are inconsistent, the verification is failed, and the connection cannot be established. If the results are consistent, the verification is successful, and connection requests from the mobile terminal are allowed, so that the connection is established. A second result signal is sent to the mobile terminal to prompt the mobile terminal about establishment of a network connection.

[0072] In step S208, the router clears all connection information generated by the connection after the connection is established.

[0073] After the connection is successful, the router may clear the dynamic password of the connection and information related to the connected mobile terminal. The master keys, temporary keys, device identification addresses, and random numbers of the mobile terminal generated by such connection are cleared so that the mobile terminal cannot automatically establish a new connection when it enters the WiFi area next time.

[0074] See FIG. 5, which is a flowchart of a second embodiment of the mobile terminal network connection method of the present application. The steps S501 and S502 are respectively the same as S401 and S402 in FIG. 4, and will not be explained here.

[0075] In step S503, the mobile terminal generates a second master key according to the second dynamic password.

[0076] The mobile terminal sends a first request signal to the server after recognizing the image information of the router, and the server sends a second dynamic password to the mobile terminal upon receiving the first request signal. The mobile terminal generates a second master key by substituting the second dynamic password into a hash function of: PMK = PBKDF2_SHAl (dynamic password, SSID, SSID length, 4096), where PMK denotes a master key, SSID denotes a router address, and PBKDF2_SHAl is a hash function.

[0077] PMK is a symmetric key that the applicant (i.e., the mobile terminal) and the authenticator (i.e., the router) can share a symmetric key called a pair of master keys, which is used to control the signal access between the two. According to the embodiment of the application, the PMK comes from the password, and in other embodiments, the PMK can be dynamically specified.

[0078] In step S504: the mobile terminal receives a first random number from the router and generates a second random number.

[0079] The first random number and the second random number, in one embodiment, are respectively identical to the fourth random number and the third random number. Specifically, the first random number and the fourth random number are random numbers generated by the router, the second random number and the third random number are random numbers generated by the mobile terminal, and all the random numbers can only be used once in the process for calculating and generating the temporary keys.

[0080] In step S505, the mobile terminal generates a first temporary key according to the first random number, the second random number, and the second master key.

[0081] The first temporary key is generated according to the first random number, the second random number, and the second master key in a pseudo-random function as below:

$$PTK = PRF\text{-}X\ (PMK,\ \text{"pairwise key expansion"}),\ Min(AA,\ SA) \parallel Max(AA,\ SA) \parallel Min(ANonce,\ SNonce) \parallel Max(ANonce,\ SNonce)),$$

where PTK denotes the temporary key, ANonce denotes the random number generated by the router, SNonce denotes the random number generated by the mobile terminal, AA denotes the identification address of the router, SA denotes the identification address of the mobile terminal, PRF-X denotes a pseudo-random function, and pairwise key expansion is a constant string.

[0082] It should be noted that when the router sends the first random number to the router, it includes the Media Access Control or Medium Access Control (MAC) address of the mobile terminal, which is translated into media access control or physical address, hardware address, for defining the location of network equipment. In the Open System Interconnection/Open System Interconnection Reference Model (OSI/RM), the third network layer is responsible for the IP address and the second layer data link is responsible for the MAC address. Therefore, a host has a MAC address, and each network location has an IP address dedicated to it. The MAC address is determined by the network card and is fixed. The MAC address is the aforementioned identification address.

[0083] In step S506, the mobile terminal generates a third random number and sends the third random number and the first temporary key to the router.

[0084] After calculating the first temporary key, the mobile terminal generates a third random number and sends the third random number to the router, which contains the MAC address of the mobile terminal, that is, the identification address.

[0085] In step S507, a second result signal is received from the router.

[0086] After receiving the third random number, the router calculates the second temporary key, compares the second temporary key with the first temporary key, establishes a connection after the comparison is matched, and sends the second result signal to the mobile terminal, and the mobile terminal confirms that the connection is established when the second signal is received.

[0087] The scheme proposed in this embodiment is summarized as follows. The mobile terminal recognizes the image information of the router, sends the first request signal to the server, receives the second dynamic password from the server, and generates the second master key according to the second dynamic password. The router receives the first dynamic password from the server and generates the first master key according to the first dynamic password, so that the router generates the first random number and sends it to the mobile terminal. The mobile terminal generates a second random number after receiving the first random number, and generates a first temporary key according to the first random number, the second random number, and the second master key. The mobile terminal generates a third random number and sends the third random number and the first temporary key to the router, and the router generates

the fourth random number after receiving the third random number. The second temporary key is generated according to the third random number, the fourth random number, and the first master key. After the second temporary key is generated, the second temporary key is matched with the first temporary key. After the comparison is matched, the connection is established, and all connection information generated by this connection is cleared after the connection is established, so that the mobile terminal cannot automatically establish a new connection when it enters the WiFi area next time.

[0088] See FIG. 3 for a flowchart of a third embodiment of the router network connection method of the present application. Compared with the second embodiment shown in FIG. 2, the differences are found after comparing the second temporary key with the first temporary key in step S206. The steps are shown below.

[0089] In step S307, if the comparison is matched, the router sends the second temporary key to the mobile terminal.

[0090] After the router successfully compares the first temporary key and the second temporary key, the second temporary key is sent to the mobile terminal.

[0091] In step S308, the router receives an authentication confirmation message from the mobile terminal, establishes a connection, and sends a third result signal to the mobile terminal.

[0092] After the mobile terminal receives the second temporary key, it compares the second temporary key with the first temporary key again. If the comparison is not matched, the connection is failed. If the comparison is matched, the authentication confirmation message is sent to the router. After receiving the confirmation message, the router establishes the connection and sends a third result signal to the mobile terminal to prompt the mobile terminal to about the connection results.

[0093] In step S309: the router clears all connection information generated by the connection after the connection is established.

[0094] After the connection is successful, the router may clear the dynamic password of the connection and all information relevant to the connected mobile terminal. All the master keys, temporary keys, device identification addresses, and random numbers of the mobile terminal generated by such connection are cleared, so that the mobile terminal cannot automatically establish a new connection when the mobile terminal enters the WiFi area next time.

[0095] See FIG. 6 for the flowchart of a third embodiment of the mobile terminal network connection method of the present application. Compared with the second embodiment shown in FIG. 5, the difference is shown after generating a third random number and sending the third random number and the first temporary key to the router in step S506, as below.

[0096] In step S607, the terminal device receives a second temporary key from the router.

[0097] The router sends the second temporary key to the mobile terminal after successfully comparing the second temporary key with the first temporary key.

[0098] In step S608, the terminal device compares the second temporary key with the first temporary key.

[0099] After receiving the second temporary key from the router, the mobile terminal compares the second temporary key with the first temporary key. When the comparison is not matched, the connection is failed.

[0100] In step S609, when the comparison is matched, an authentication confirmation message is sent to the router.

[0101] The mobile terminal compares the second temporary key with the first temporary key, and sends an authentication confirmation message to the router to prompt the router that the authentication is confirmed.

[0102] In step S610: the mobile terminal receives the third result signal from the router.

[0103] The router establishes a connection after receiving the authentication confirmation message sent by the mobile terminal, and sends a third result signal to the mobile terminal to prompt that the mobile terminal is connected successfully.

[0104] Compared with the second embodiment (FIGs. 2 and 5), the differences are as summarized. The router compares the second temporary key, and after the comparison is matched, the router sends the second temporary key to the mobile terminal, and the mobile terminal then compares the second temporary key with the first temporary key once, and after the comparison is successful, an authentication confirmation message is sent to the router, the router allows the mobile terminal to connect after receiving the authentication confirmation message, and sends the first connection after the connection is established. The third result signal is sent to the mobile terminal to prompt the mobile terminal that the connection is established. In this embodiment, two comparisons are performed to further improve the security of the network connection. The router clears all connection information generated by the connection after the connection is established, so that the mobile terminal cannot automatically establish a new connection when the mobile terminal enters the WiFi area next time.

[0105] Please refer to FIG. 7 for a structural diagram of signal transmission of mobile terminal and router in the present application. Specifically, the mobile terminal 11 recognizes the image information of the router 12 and sends a first request signal to the server 13. After receiving the first request signal, the server 13 sends a first dynamic password to the router 12 and a second dynamic password to the mobile terminal 11. The mobile terminal 11 generates a second master key according to the second dynamic password, and the router 12 generates a first random number and sends the first random number to the mobile terminal 11. The mobile terminal 11 generates a second random number, and generates a first temporary key according to the first random number, the second random number, and the second

master key. The first temporary key is then sent to the router 12 for verification. The router 12 receives a third random number and the first temporary key from the mobile terminal, generates a fourth random number, and then generates a second temporary key according to the third random number, the fourth random number, and the first master key. The router 12 then compares the second temporary key with the first temporary key. If the comparison is matched, the router 12 sends the second temporary key to the mobile terminal 11, and the mobile terminal 11 sends an authentication confirmation message to the router 12 after verifying the second temporary key with the first temporary key. The router 12 establishes a connection after receiving the authentication confirmation message, and sends a result signal to the mobile terminal 11 prompting the successful connection establishment.

[0106] Please refer to FIG. 8, which is a structural diagram of the mobile terminal or router of the present application. The mobile terminal or router comprises a processor 51 and a memory 52 coupled to the processor 51.

[0107] The memory 52 stores program data executable by the processor 51 to carry out the connection method as described in any of the aforementioned embodiments.

[0108] The processor 51 is configured to load and execute the program data stored in the memory 52.

[0109] The processor 51 is also referred to as the central processing unit (CPU). The processor 51 may be an integrated circuit chip with signal processing capability. The processor 51 may also be a general-purpose processor, a digital signal processor (DSP), an ASIC, a ready-made programmable gate array (FPGA), or other programmable logic devices, discrete gate, or transistor logic devices, and discrete hardware components. The general processor can be a microprocessor or the processor can be any conventional processor, etc.

[0110] The memory 52 can be a memory module, a TF card, etc., which can store all the information in the mobile terminal, comprising the input original data, computer programs, intermediate operation results, and final operation results. It stores and takes out information according to the position designated by the controller. With the memory, the mobile terminal has the memory function and can ensure normal operations. The memory of mobile terminal can be divided into main memory and auxiliary memory (external memory) according to the purpose memory, and also can be classified into external memory and internal memory. The external storage is usually magnetic medium or optical disk, which can store information for a long time. The memory refers to the storage unit on the motherboard, which is used to store the currently executing data and programs. However, it is only used for temporary storage of programs and data. If the power is turned off or power outage occurs, the data may be lost.

[0111] The mobile terminal or router also comprises other devices, which are the same as other devices and functions in the mobile terminal or router in the prior art, and will not be repeated here.

[0112] Refer to FIG. 9, a structural diagram of an embodiment of a storage medium of the present application is shown. The storage medium of the present application stores program data 61 executable by the processor to carry out the connection methods as described in the aforementioned embodiments. The program data 61 can be stored in the storage medium in the form of software products, comprising a number of instructions to enable a computer device (which may be a personal computer, a server, or a network device, etc.) or a processor to execute all or part of the steps of the methods described in the various embodiments of the present application. The storage devices mentioned above may include: U disk, mobile hard disk, read-only memory (ROM), random access memory (RAM), disk or CD, and other media that can store program code, or terminal equipment such as computer, server, mobile phone, tablet, etc.

[0113] In the several embodiments provided by this application, it should be understood that the disclosed system, device, and method can be realized in alternative ways. For example, the embodiments of the device described above is only schematic. For example, the definitions of modules or units are merely based on logical functions. In actual implementation, there may be other ways to define the units, for example, multiple units or components can be combined or integrated into another system, or some features can be ignored or not implemented. On the other hand, the mutual coupling or direct coupling or communication connection shown or discussed may be indirect coupling or communication connection through some interfaces, devices, or units, and may be in the form of electrical, mechanical, or other forms.

[0114] In addition, each functional unit in each embodiment of the present application can be integrated into a processing unit, or each unit may exist independently, or two or more units may be integrated in one unit. The integrated unit can be implemented in the form of hardware or software function unit.

[0115] The above embodiments are merely illustrative implementations of the application, and are not intended to limit the scope of the patent of the application. All equivalent structure or equivalent process transformation made by using the description and drawings of the application, or directly or indirectly applicable to other related technical fields, are similarly included in the scope of patent protection of the application.

Claims

1. A network connection method applicable to a router, **characterized in that** the method comprises following steps:

the router receiving a first dynamic password from a server;
the router receiving a second dynamic password from a mobile terminal and comparing the second dynamic password with the first dynamic password;
when the comparison is matched, establishing a connection, and sending a first result signal to the mobile terminal; and
the router clearing connection information generated by the connection after the connection is established.

2. The network connection method according to claim 1, **characterized in that** after the step of the router receiving the first dynamic password from the server, the network connection method further comprises:

the router generating a first master key according to the first dynamic password;
the router generating a first random number and sending the first random number to the mobile terminal;
receiving a third random number and a first temporary key from the mobile terminal and
generating a fourth random number;
generating a second temporary key according to the third random number, the fourth random number, and the first master key;
comparing the second temporary key with the first temporary key; and
when the comparison is matched, establishing the connection, and sending a second result signal to the mobile terminal.

3. The network connection method according to claim 2, **characterized in that** the step of comparing the second temporary key with the first temporary key further comprises:

when the comparison is matched, the router sending the second temporary key to the mobile terminal; and
the router receiving an authentication confirmation message from the mobile terminal, establishing the connection, and sending a third result signal to the mobile terminal.

4. The network connection method according to claim 2, **characterized in that** the step of the router generating the first master key by substituting the first dynamic password into a hash function PBKDF2_SHA1:

PMK=PBKDF2_SHA1 (dynamic password, SSID, SSID length, 4096);
wherein PMK denotes a master key and SSID denotes an address of the router; and
the step of generating the second temporary key according to the third random number, the fourth random number, and the first master key is based on a pseudo-random function PRF-X:

$$PTK = PRF\text{-}X\ (PMK,\ \text{“Pairwise key expansion”},\ Min(AA,SA)\ ||\ Max(AA,SA)\ ||\ Min(ANonce, SNonce)\ ||\ Max(ANonce, SNonce));$$

wherein PTK denotes a temporary key, ANonce denotes a random number generated by the router, SNonce denotes a random number generated by the mobile terminal, AA denotes an identification address of the router, SA denotes an identification address of the mobile terminal, and the "Pairwise key expansion" denotes a constant character string.

5. The network connection method according to claim 1, **characterized in that** the first dynamic password is a digital password or a combination of numbers and letters.

6. The network connection method according to claim 1, **characterized in that** the second dynamic password is assigned to the mobile terminal by the server.

7. A network connection method applicable to a mobile terminal, **characterized in that** the method comprises following steps:

the mobile terminal recognizing an image information from a router and sending a first request signal to a server when the image information is successfully recognized;
receiving a second dynamic password from the server;
sending a second dynamic password to the router; and

receiving a first result signal from the router.

8. The network connection method according to claim 7, **characterized in that** after the step of receiving the second dynamic password from the server, the network connection method further comprises:

the mobile terminal generating a second master key according to the second dynamic password;
receiving a first random number from the router and generating a second random number; generating a first temporary key according to second dynamic password, the second random number, and the second master key;
generating a third random number and sending the third random number and the first temporary key to the router; and
receiving a second result signal from the router.

9. The network connection method according to claim 8, **characterized in that** after the step of generating the third random number and sending the third random number and the first temporary key to the router, the network connection method also comprises:

receiving a second temporary key from the router;
comparing the second temporary key with the first temporary key;
sending an authentication confirmation message to the router when the comparison is matched; and
receiving a third result signal from the router.

10. The network connection method according to claim 7, **characterized in that** the image information comprises an identification code.

11. The network connection method according to claim 7, **characterized in that** the first dynamic password is a digital password or a combination of numbers and letters.

12. A mobile terminal, comprising a memory and a processor interconnected with each other, wherein the memory stores program data loadable and executable by the processor to carry out following steps:

the mobile terminal recognizing an image information from a router and sending a first request signal to a server when the image information is successfully recognized, wherein
the image information comprises an identification code;
receiving a second dynamic password from the server;
sending the second dynamic password to the router; and
receiving a first result signal from the router.

13. The mobile terminal according to claim 12, **characterized in that** after the step of
receiving the dynamic password from the server, the mobile terminal also comprises:

the mobile terminal generating a second master key according to the second dynamic password;
receiving a first random number from the router and generating a second random number;
generating a first temporary key according to the first random number, the second random number, and the second master key ;
generating a third random number and sending the third random number and the first temporary key to the router; and
receiving a second result signal from the router.

14. The mobile terminal according to claim 13, **characterized in that** after the step of generating the third random number and sending the third random number and the first temporary key to the router, the mobile terminal further performs following steps:

receiving a second temporary key from the router;
comparing the second temporary key with the first temporary key;
sending an authentication confirmation message to the router when the comparison is matched; and
receiving a third result signal from the router.

15. The mobile terminal according to claim 12, **characterized in that** the first dynamic password is a digital password

or a combination of numbers and letters.

16. A router, comprising a memory and a processor interconnected with each other, wherein the memory stores program data loadable and executable by the processor to carry out following steps:

the router receiving a first dynamic password from a server;
the router receiving a second dynamic password from a mobile terminal and comparing the second dynamic password with the first dynamic password, wherein the second dynamic password is assigned to the mobile terminal by the server;
when the comparison is matched, establishing a connection, and sending a first result signal to the mobile terminal; and
the router clearing connection information generated by the connection after the connection is established.

17. The router according to claim 16, **characterized in that** after receiving the first dynamic password from the server, the router performs following steps:

generating a first master key according to the first dynamic password;
generating a first random number and sending the first random number to the mobile terminal;
receiving a third random number and a first temporary key from the mobile terminal and generating a fourth random number;
generating a second temporary key according to the third random number, the fourth random number, and the first master key;
comparing the second temporary key with the first temporary key; and
when the comparison is matched, establishing the connection, and sending a second result signal to the mobile terminal.

18. The router according to claim 17, **characterized in that** after comparing the second temporary key with the first temporary key, the router further performs following steps:

when the comparison is matched, sending the second temporary key to the mobile terminal; and
receiving an authentication confirmation message from the mobile terminal, establishing the connection, and sending a third result signal to the mobile terminal.

19. The router according to claim 17, **characterized in that** the router generates the first master key by substituting the first dynamic password into a hash function PBKDF2_SHA1:

PMK=PBKDF2_SHA1 (dynamic password, SSID, SSID length, 4096);
wherein PMK denotes a master key and SSID denotes an address of router; and
the step of generating the second temporary key according to the third random number, the fourth random number, and the first master key is as follows:

$$PTK = PRF\text{-}X\ (PMK,\ \text{“Pairwise key expansion”},\ Min(AA,SA)\ ||\ Max(AA,SA)\ ||\ Min(ANonce,SNonce)\ ||\ Max(ANonce,SNonce));$$

wherein PTK denotes a temporary key, ANonce denotes a random number generated by the router, SNonce denotes a random number generated by the mobile terminal, AA denotes an identification address of the router, SA denotes an identification address of the mobile terminal, PRF-X denotes a pseudo-random function, and the "Pairwise key expansion" denotes a constant character string.

20. The router according to claim 16, **characterized in that** the first dynamic password is a digital password or a combination of numbers and letters.

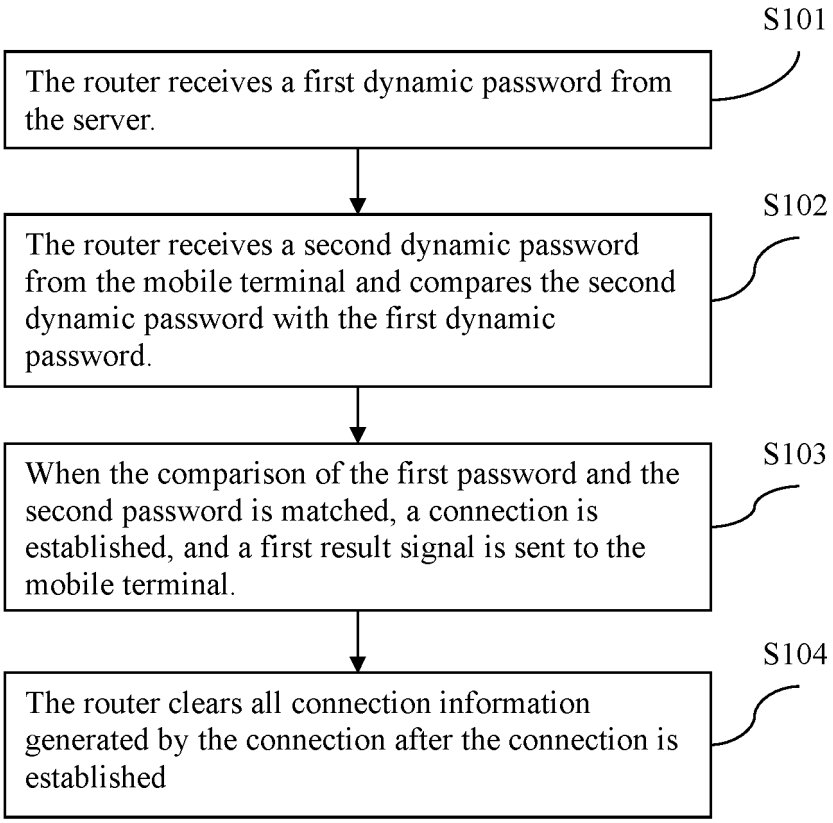
S101
The router receives a first dynamic password from the server.
S102
The router receives a second dynamic password from the mobile terminal and compares the second dynamic password with the first dynamic password.
S103
When the comparison of the first password and the second password is matched, a connection is established, and a first result signal is sent to the mobile terminal.
S104
The router clears all connection information generated by the connection after the connection is established

FIG. 1

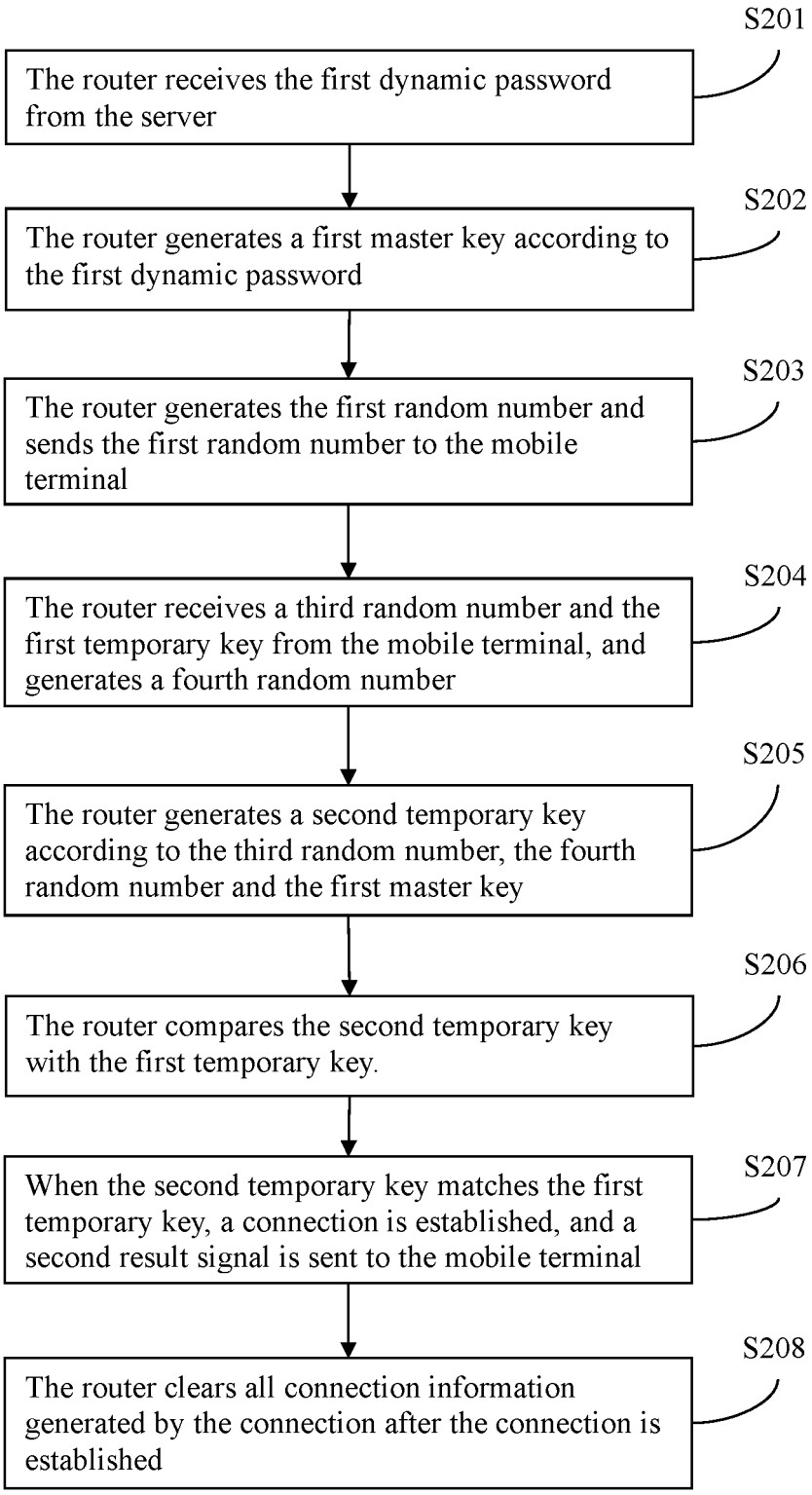
S201
The router receives the first dynamic password from the server
S202
The router generates a first master key according to the first dynamic password
S203
The router generates the first random number and sends the first random number to the mobile terminal
S204
The router receives a third random number and the first temporary key from the mobile terminal, and generates a fourth random number
S205
The router generates a second temporary key according to the third random number, the fourth random number and the first master key
S206
The router compares the second temporary key with the first temporary key.
S207
When the second temporary key matches the first temporary key, a connection is established, and a second result signal is sent to the mobile terminal
S208
The router clears all connection information generated by the connection after the connection is established

FIG. 2

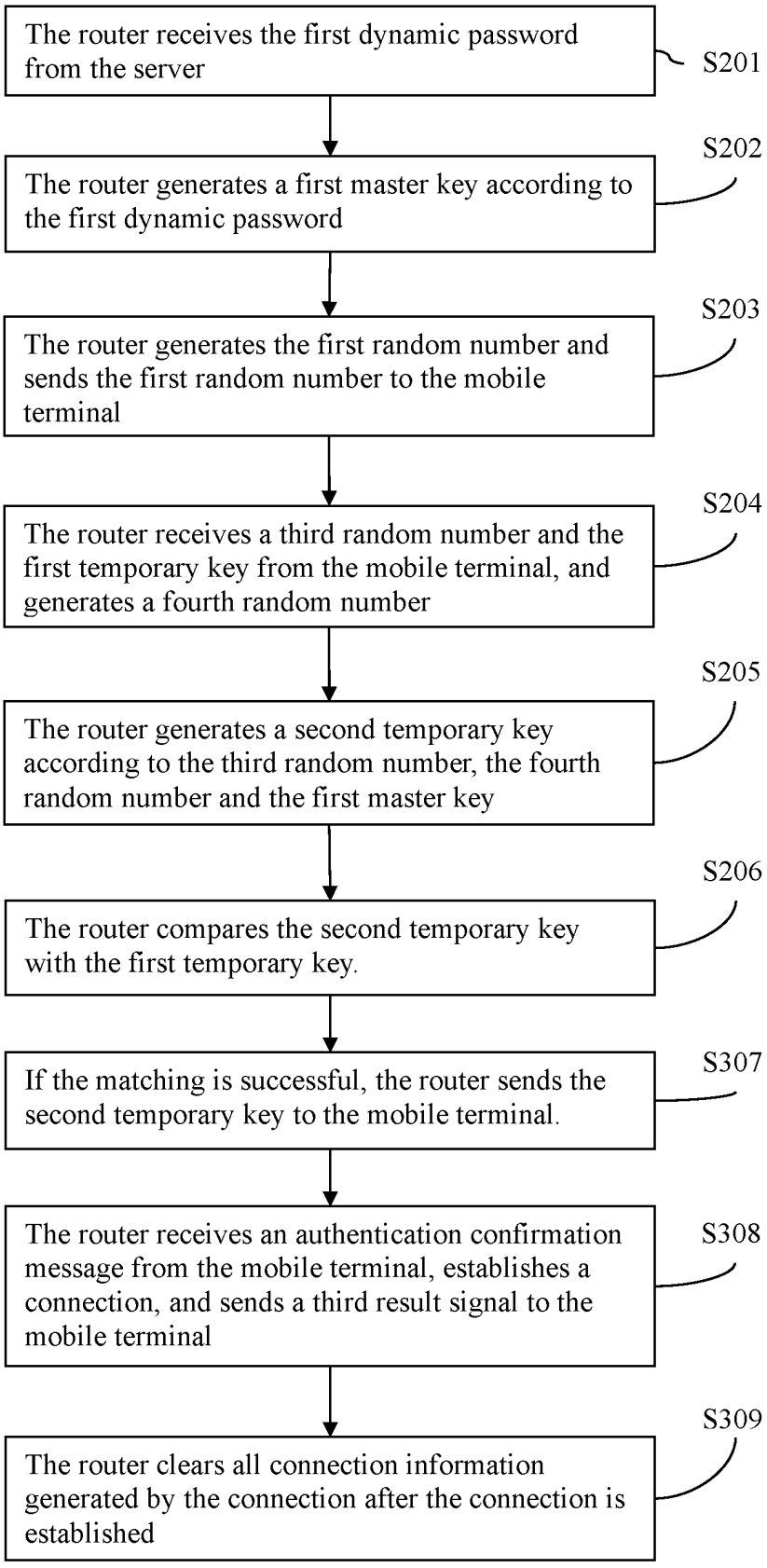
The router receives the first dynamic password from the server
S201
The router generates a first master key according to the first dynamic password
S202
The router generates the first random number and sends the first random number to the mobile terminal
S203
The router receives a third random number and the first temporary key from the mobile terminal, and generates a fourth random number
S204
The router generates a second temporary key according to the third random number, the fourth random number and the first master key
S205
The router compares the second temporary key with the first temporary key.
S206
If the matching is successful, the router sends the second temporary key to the mobile terminal.
S307
The router receives an authentication confirmation message from the mobile terminal, establishes a connection, and sends a third result signal to the mobile terminal
S308
The router clears all connection information generated by the connection after the connection is established
S309

FIG. 3

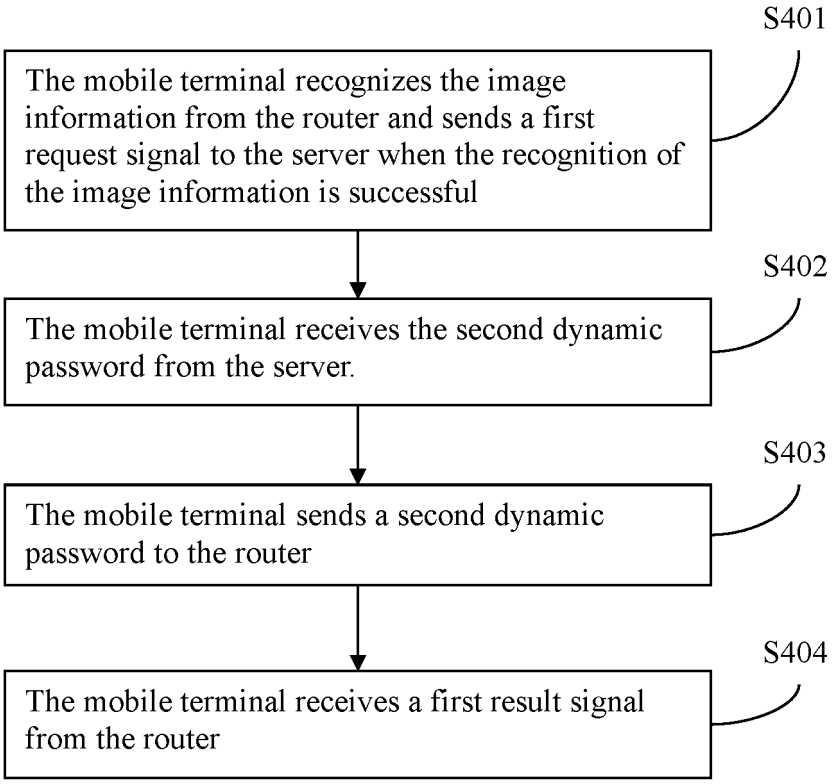
S401
The mobile terminal recognizes the image information from the router and sends a first request signal to the server when the recognition of the image information is successful
S402
The mobile terminal receives the second dynamic password from the server.
S403
The mobile terminal sends a second dynamic password to the router
S404
The mobile terminal receives a first result signal from the router

FIG. 4

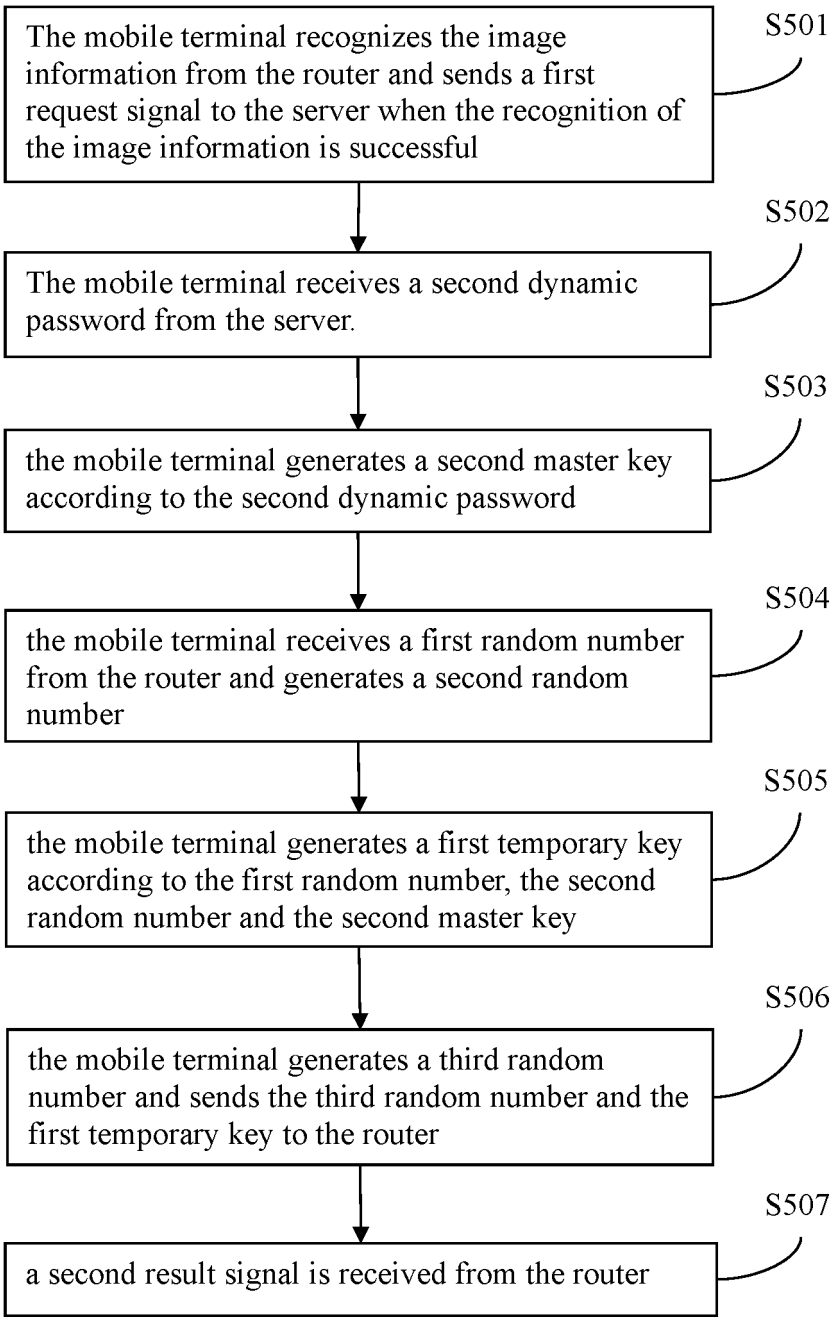
The mobile terminal recognizes the image information from the router and sends a first request signal to the server when the recognition of the image information is successful
S501
The mobile terminal receives a second dynamic password from the server.
S502
the mobile terminal generates a second master key according to the second dynamic password
S503
the mobile terminal receives a first random number from the router and generates a second random number
S504
the mobile terminal generates a first temporary key according to the first random number, the second random number and the second master key
S505
the mobile terminal generates a third random number and sends the third random number and the first temporary key to the router
S506
a second result signal is received from the router
S507

FIG. 5

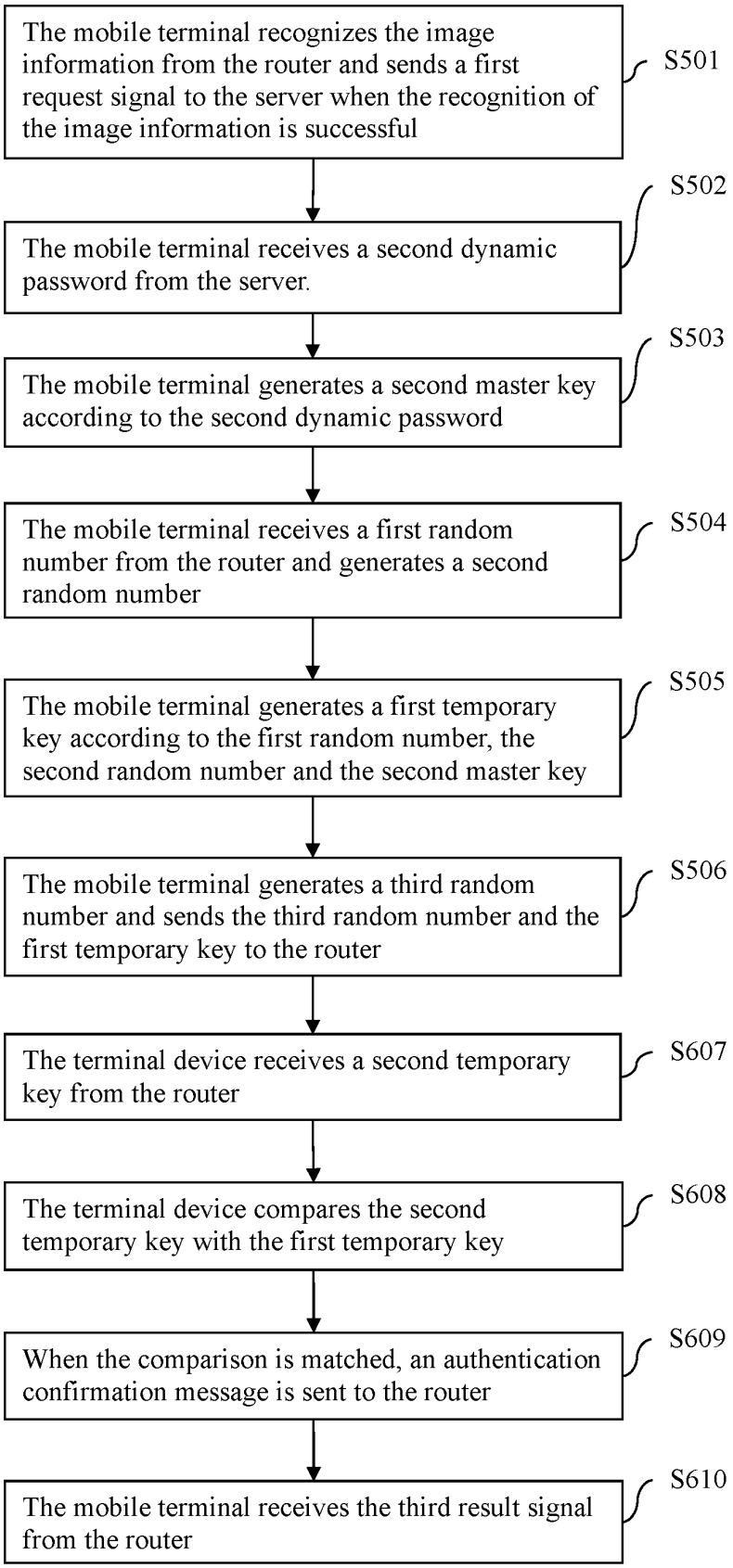
The mobile terminal recognizes the image information from the router and sends a first request signal to the server when the recognition of the image information is successful
S501
The mobile terminal receives a second dynamic password from the server.
S502
The mobile terminal generates a second master key according to the second dynamic password
S503
The mobile terminal receives a first random number from the router and generates a second random number
S504
The mobile terminal generates a first temporary key according to the first random number, the second random number and the second master key
S505
The mobile terminal generates a third random number and sends the third random number and the first temporary key to the router
S506
The terminal device receives a second temporary key from the router
S607
The terminal device compares the second temporary key with the first temporary key
S608
When the comparison is matched, an authentication confirmation message is sent to the router
S609
The mobile terminal receives the third result signal from the router
S610

FIG. 6

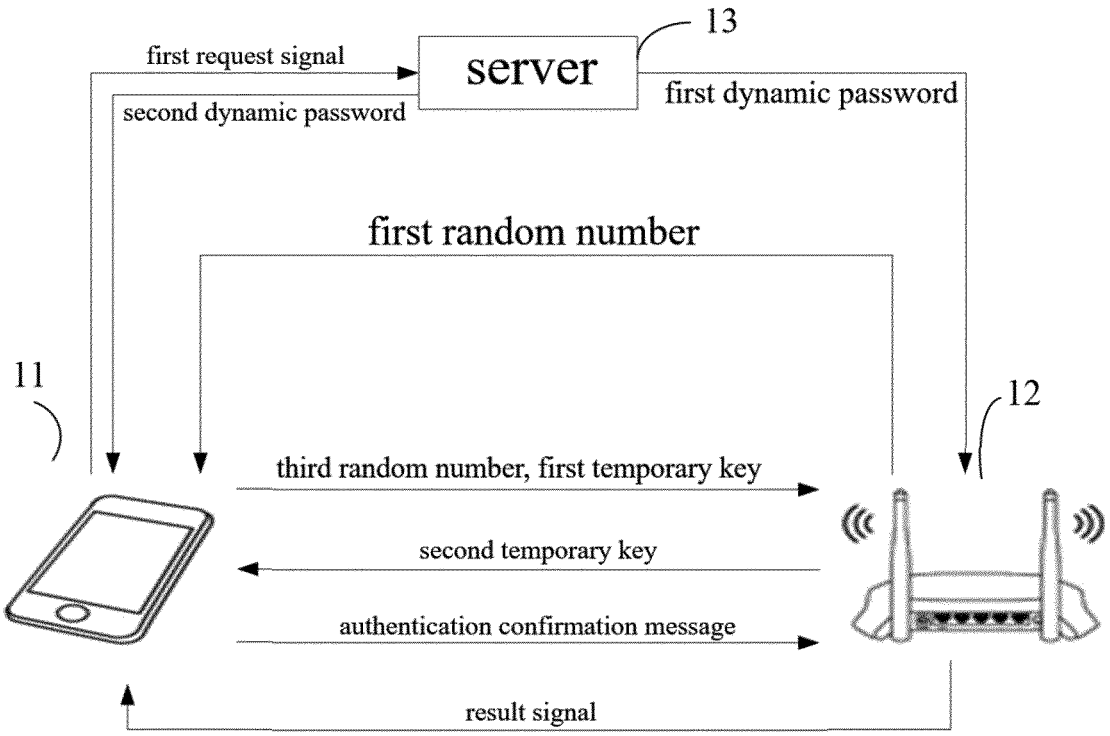
13
server
first request signal
second dynamic password
first dynamic password
first random number
11
12
third random number, first temporary key
second temporary key
authentication confirmation message
result signal

FIG. 7

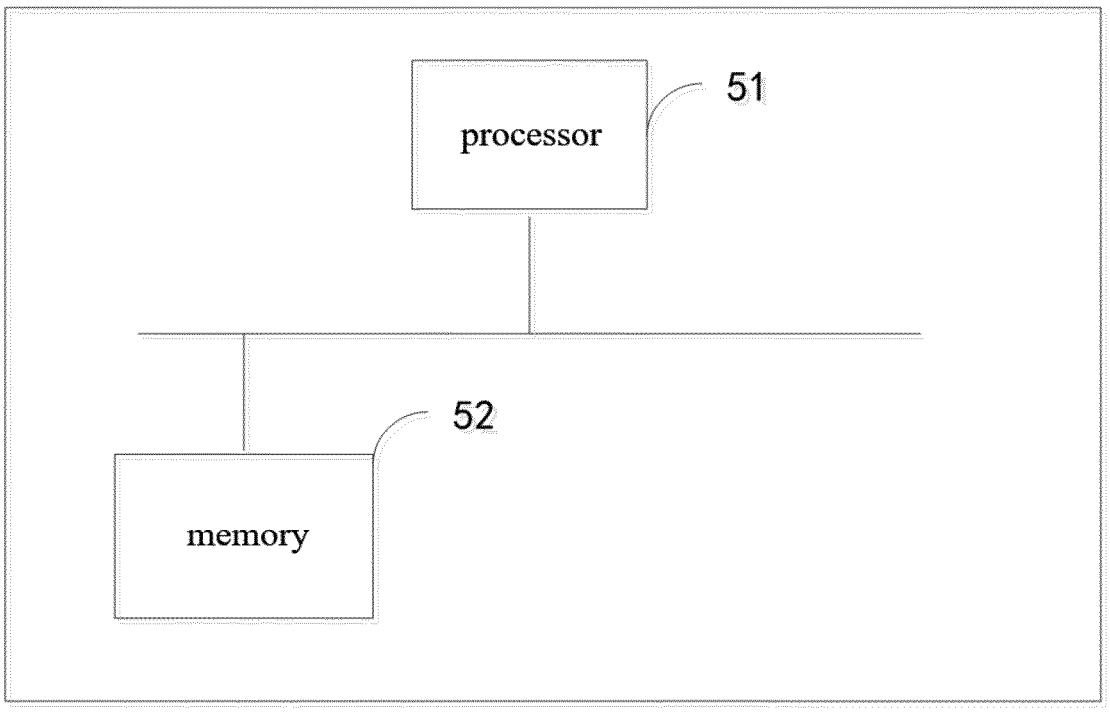
processor
51
52
memory

FIG. 8

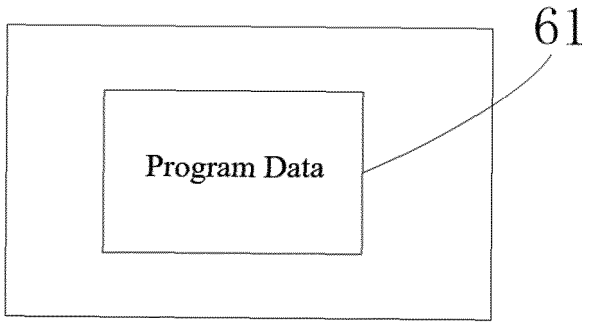

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/125051

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i; H04W 12/08(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 手机, 移动终端, PAD, 局域网, 热点, 路由器, 服务器, 第一, 第二, 密码, 密钥, 校验, 验证码, 图形, 二维码, 匹配, 比对, 验证, 连接, 链接, 清除, 释放, wifi, hot, wlan, router, terminal, mobile, match, compar+, key, authentic+, verif+, releas+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110213760 A (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD.) 06 September 2019 (2019-09-06) claims 1-10	1-20
X	CN 104394533 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED) 04 March 2015 (2015-03-04) abstract, description, paragraphs 40-61, and figures 1 and 2	7, 10-12, 15
Y	CN 104394533 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED) 04 March 2015 (2015-03-04) abstract, description, paragraphs 40-61, and figures 1 and 2	1, 5, 6, 16, 20
Y	CN 108111522 A (WUHAN YANGTZE OPTICAL TECHNOLOGY CO., LTD.) 01 June 2018 (2018-06-01) abstract	1, 5, 6, 16, 20
A	CN 106412897 A (XI'AN HANJU NETWORK TECHNOLOGY CO., LTD.) 15 February 2017 (2017-02-15) entire document	1-20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 February 2020	**12 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/125051

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015089324 A1 (NANTMOBILE, LLC) 18 June 2015 (2015-06-18) entire document	1-20

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/125051

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110213760 A	06 September 2019	None	
CN 104394533 A	04 March 2015	None	
CN 108111522 A	01 June 2018	None	
CN 106412897 A	15 February 2017	None	
WO 2015089324 A1	18 June 2015	US 2015302571 A1	22 October 2015

Form PCT/ISA/210 (patent family annex) (January 2015)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 201910355810 **[0001]**